IN THE SPECIFICATION:

On page 5 line 6, after "(LAN) 105". Insert -- "Server 112 includes a known CPU 150, operating system 152, memory 154 and hard drive storage 156."--.

The paragraph should read:

The present invention will now be described in detail with reference to the figures. Figure 1 illustrates a distributed computer system generally designated 100. System 100 comprises a firewall or router 110, a server 112 coupled to the firewall or router 110 in a subnet 103, and a multiplicity of client/user computers such as computer 114 coupled to server 112 via a Local Area Network (LAN) 105. Server 112 includes a known CPU 150, operating system 152, 154 and hard drive storage 156. The firewall or router 110 performs typical functions of known firewalls such as blocking e-mails with Source Addresses (SAs) known to be currently malicious. In addition, firewall or router 110 also includes a spam filter program 119 which reviews each incoming e-mail and ascertains from its header its source IP address, i.e. the IP address of the sender of the e-mail. The firewall or router 110 includes a set of filter rules 117 each defined to block e-mail from a respective IP address or range of IP addresses (typically for a finite period of time). So, if the IP address of the sender of the e-mail matches one of the filter rules (and the filter rule is still in effect), then the firewall or router 110 "blocks" the e-mail, i.e. prevents it from passing through to the server 112. The example of Figure 1 illustrates four filter rules (SA1, SA2, SA3 and SA4) in firewall or router 110. Each of the filter rules blocks e-mails from a respective range of source IP addresses (for a finite period of time).

IN THE SPECIFICATON:

On page 5 line 17 after "message transfer agent ("MTA") 129," insert --"in storage 156"--.

On page 5 line 21 after "spam detector program" insert --"in storage 156"--.

The paragraph should read as follows:

The server 112 includes a message transfer agent ("MTA") 129 in storage 156, i.e. a program function which forwards e-mail, determined not to be spam, received from the firewall or router 110 to the intended recipient/user. For example, MTA 129 can be that of Postfix (trademark of Postfix Corporation) program. The server 112 also includes a known spam detector 121 such as "Spam Assassin" spam detector program in storage 156. The spam detector 121 may be part of the MTA 129 or a separate program. The spam detector reviews incoming e-mail to detect when the same e-mail (i.e. the same or substantially the same text) is addressed to multiple different recipients/users. The spam detector may ignore e-mails sent from bona fide correspondents, such as employees of a corporation to which the e-mails are sent, such that these e-mails are not considered to be spam. The "bona fide correspondents" may be recorded on a list accessible to the spam detector. But, the same e-mails sent from another entity to multiple recipients/users are assumed to be spam. The user computer 114 may also include an optional spam detector program 123 which identifies spam based on host-based screening software or preferences of the user. The source IP addresses identified by this optional spam detector program 123 result in additional filter rules (each blocking e-mail from a single IP address or range of IP addresses) that can be applied at the firewall or router 110.

IN THE SPECIFICATION:

On page 8 line 5 after "may reside" insert --"in storage 156"--.

The paragraph should read as follows:

The range finder program 130 may reside in storage 156 in server 112 or in another server coupled to server 112 by a network. The range finder program 130 is also coupled by a network to an existing/known Internet service company called "Internet Assigned Number Authority" company or "IANA" 138 (or a similar Internet service). IANA 138 currently maintains a database of all (that is, the range 60.70.80.0 through 60.70.80.127) addresses and the entity that "owns" or registers each block of IP addresses. IANA 138 obtains its IP address ownership information based on the following process. Each entity that desires to use an IP source address on the Internet must first register it with IANA. After the spam detector 121 or spam detector 123 notifies the range finding program 130 of a suspected spammer's source IP address, the range finder program 130 contacts "IANA" (or a similar Internet service) by e-mail and supplies the source IP address of the suspected spammer. (In the example of Figure 1, the range finder program supplies source IP addresses SA5 and SA6 to IANA, although the notification of each source IP address can be done at different times.) The range finding program 130 also asks IANA to state who owns each source IP address and what other IP addresses are owned by this same entity (step 208). IANA supplies the requested information from its registration database. (In the example illustrated in Figure 1, IANA returns a range of source IP addresses owned/registered by the registrant of SA5, and a range of source IP addresses owned/registered by the registrant of SA6.) After receiving the information from IANA, the ranger finder program defines ranges of source IP addresses from which e-mail should be blocked (step 212). Each "range" is a list of all the IP addresses owned by the owner of the source IP address identified as a spammer by the spam detector in step 204. Because the entire range will be blocked, and not just the source IP address of the single spam e-mail, this will thwart/block a spammer who shifts to another of its registered source IP addresses to send new spam. The "range" can be a sequential range of source IP addresses or a grouping of non-sequential source IP addresses, as

the case may be. Alternately, the blocked range can be limited to a smaller range of addresses that contains the detected source IP address and are owned by the owner of the spam e-mail, where the smaller range is a size typically used for spamming, such as a range of thirty two addresses for example, 60.70.80.0 through 60.70.80.31. In another embodiment of the present invention, the range finding program 130 determines the range of blocked source IP addresses as a range of addresses (such as 60.70.80.0 through 60.70.80.256) that contain the source IP address of the spam and are not within the set of source IP addresses known by the manager of the computer system to be of interest.

IN THE SPECIFICATION:

On page 9 line 11 before "in server 112 or another server" insert --"in storage 156"--.

Next, the range finding program 130 passes the ranges of blocked, source IP addresses to monitor program 132. (In the example illustrated in Figure 1, there is one range for source IP address SA5 and another range for source IP address SA6.) The monitor program 132 can reside in storage 156 in server 112 or another server which contains the range finder program 130 (if the range finder program 130 does not reside on server 112). Then, the monitor program 132 creates the filter rule(s) to be used by firewall or router 110 (step 220). The filter rule(s) specifies the range of blocked, source IP addresses obtained from the range finder program 130. For the filter rule(s), the monitor program 132 also specifies a start time to begin enforcing the filter rule and a duration/period for enforcing the filter rule as described above.